



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

*Am*

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/834,084	04/11/2001	Michael S. Fox	42390P11074	2761

8791 7590 03/25/2005

BLAKELY SOKOLOFF TAYLOR & ZAFMAN  
12400 WILSHIRE BOULEVARD  
SEVENTH FLOOR  
LOS ANGELES, CA 90025-1030

EXAMINER
----------

PICH, PONNOREAY

ART UNIT	PAPER NUMBER
----------	--------------

2135

DATE MAILED: 03/25/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

Application No.

09/834,084

Applicant(s)

FOX ET AL.

Examiner

Ponnoreay Pich

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 3/3/2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-28 is/are pending in the application.
- 4a) Of the above claim(s) 2, 6, 11, 15 and 21 is/are ~~withdrawn from consideration~~ *Cancelled*.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1, 3-5, 7-10, 12-14, 16-20 and 22-28 is/are rejected.
- 7) ☒ Claim(s) 9 and 18 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- ☐ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- ☐ Notice of Informal Patent Application (PTO-152)
- ☐ Other: \_\_\_\_\_

### **DETAILED ACTION**

Claims 1, 10, 12, 17-19, and 25 have been amended by the applicant. Claims 2, 6, 11, 15, and 21 were cancelled. Claims 1, 3-5, 7-10, 12-14, 16-20, and 22-28 are pending. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

### ***Response to Arguments***

Applicant's arguments filed on 3/3/2005 have been fully considered but they are not persuasive. The applicant argues that on page 7, lines 8-11 of the Office action dated 1/13/2005 Stefik does not teach at col 3, lines 34-50 presenting a challenge code to a user of the application program, requiring the user to obtain a passcode in response to the challenge code, and determining validity of the passcode, and performing the recalculating and copying only when the passcode is valid. What the examiner actually recited was that "Stefik teaches presenting a challenge code to a user of the application program, requiring the user to obtain a passcode in response to the challenge code, and determining validity of the passcode." The examiner agrees with the applicant that the recited text refers to US patent 5,247,575 by Sprague. However, the examiner never stated that Stefik teaches the recited limitation was disclosed *by Stefik's invention*. Instead, what Stefik teaches was that the recited limitation was known at the time the applicant's invention was made as Stefik references Sprague's invention and summarizes it in a manner which reads on the limitation recited by the examiner. Stefik teaching that a recited limitation was known in the art at the time the

applicant's invention was made is still the same thing as Stefik teaching the recited limitation for the purposes of a 103 rejection as was used by the examiner.

Note that in the cited passage that information packages are encrypted. To access the decrypted form of the information packages, keys are needed. A key is a form of a passcode as it allows for access to something. As for the challenge code, the encrypted information package itself constitutes a challenge code as the user cannot access the information in a useable format until the user obtains a valid key. The application program is of course any program that is used to access the information package. To decrypt the encrypted information package with the obtained key, the validity of the key must be determined. This determination could be as simple as trying to decrypt the information package using the key and seeing if proper decryption occurs or it could take on some other form. However, determination of the validity of the key/passcode in some form must at some point occur for the information package to be accessed in a useable format by the user. The sequence of events which occurs (i.e. the proper decryption of the information package) when a valid passcode/key is used must only occur when the passcode/key is valid or there would be no point in using such a security feature.

The applicant made the same arguments for claims 19 and 25. These arguments are also not persuasive for the same reasons given above.

### ***Response to Amendment***

The examiner note that claims 1, 10, 19, and 25 have been amended to overcome grammatical objections listed in the previous Office action. Claims 8, 10-18,

and 25-28 were rejected under 35 USC 112, second paragraph. The applicant has amended these claims also. As such, the examiner withdraws the previous objections and 112, second paragraph rejections. As these claims were amended, new grounds of rejections will be applied to the claims below including rejections based on new issues raised due to the amendments. The examiner will also make new objections and 112 rejections that arise from these amendments if any. The examiner will copy and paste the rejections for any claims which were not amended into this Office action from the previous Office action for clarity purposes. However, the applicant should note that the previous action is incorporated by reference in its entirety, including any specific indications of various claim elements which the examiner might accidentally forget to reiterate in this action. The examiner also notes and accepts the amendments to the specification and the abstract submitted by the applicant on 3/3/2005.

### ***Claim Objections***

Claims 9 and 18 are objected to because of the following informalities:

1. Claim 9 recites "The method of claim 2." However, claim 2 has been cancelled by the applicant. The examiner assumes the applicant meant "claim 1."
2. Claim 18 recites "The method of claim 11." However, claim 11 has been cancelled by the applicant. The examiner assumes the applicant meant "claim 10."

Appropriate correction is required.

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1, 3-5, 7-10, 12-14, 16-20, and 22-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fox (U.S. 5,765,172) in view of Stefik (U.S. 5,715,403) and further in view of "RFC 2104".

**Claims 1 and 10:**

Fox discloses a method of, and an article comprising a storage medium having a plurality of machine readable instructions, wherein when the machine readable instructions are executed by a processor, the machine readable instructions provide for, deterring a rollback attack against a first database comprising:

- Determining if the first database is corrupted, the first database being associated with a first authentication code (col 1, lines 65-67 and col 2, lines 1-6).
- Determining if a second database is corrupted, the second database being associated with a second authentication code, and having contents substantially the same as the first database (col 2, 2<sup>nd</sup> paragraph).

The examiner has interpreted an authentication code as any sort of hash, object, code, or checksum value associated with a database in any manner.

Fox does not teaches when the second database is not corrupted, presenting a challenge code to a user of the application program, requiring the user to obtain a passcode in response to the challenge code, and determining the validity of the

passcode, and performing the recalculating and copying only when the passcode is valid, recalculating the second authentication code using a portion of the first authentication code, copying the second database over the first database, and proceeding with authorized operations for processing content by an application program.

However, Stefik teaches presenting a challenge code to a user of the application program, requiring the user to obtain a passcode in response to the challenge code, and determining validity of the passcode (col 3, lines 34-50). Stefik disclosed that it is possible for a user to have access to selected content already, but not be able to make any practical use of the content until they contact a central accounting facility to obtain a key/passcode to unlock the selected content. **The manner in which Stefik teaches this limitation is that he discloses that this limitation was known in the art at the time the applicant's invention was made.** As mentioned, the information package being encrypted as disclosed by Stefik in his discussion of known matters in the art constitutes a challenge code as the user cannot make use of the content until he/she obtains a key/passcode to decrypt the content. It would also have been obvious to one of ordinary skill in the art to execute whatever set of processes that gets executed should a key/passcode be valid only if the key/passcode is valid or there would be no point in using the key/passcode for security purposes.

RFC 2104 teaches the use of HMAC, (Key) Hashed Message Authentication Code. RFC 2104 discloses that an authentication code using a hash or checksum, such as MD5, along with a secret key can be used to provide a way "to check the

Art Unit: 2135

integrity of information transmitted over or stored in an unreliable medium" (RFC 2104, Introduction). One advantage of using HMAC over just an ordinary checksum algorithm is that the checksum algorithm portion of a HMAC can be replaced with a more secure or reliable algorithm discovered at a later date (RFC 2104, Introduction). Used in combination with the secret key, it is also more inherently secure than an ordinary checksum.

It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the teachings disclosed by Stefik and RFC 2104 with Fox's teachings according to the limitations recited in claim 1. One of ordinary skill would have been motivated to incorporate Stefik and RFC 2104's teachings with Fox's as it would lead to better database security.

**Claims 3 and 12:**

Fox discloses a method of claim 1 further comprising, and an article of claim 10, further comprising machine readable instructions for, continuing with authorized operations of the application program for processing content when the first database is not corrupted (col 7, lines 27-41 and fig 6). One of ordinary skill would recognize that there is no point in not doing anything if the first database is not corrupt and instead would continue with ordinary operations of the application.

**Claims 4 and 13:**

Fox does not disclose the method of claim 1 and the article of claim 10, wherein the first database comprises usage rules for processing selected content by the application program, the usage rules including a copy count for the selected content.



This is, however, disclosed by Stefik (col 3, 1<sup>st</sup> paragraph; col 4, lines 4-24; and col 10 and 11, Table 1). One of ordinary skill in the art at the time of the applicant's invention would be motivated to combine the two teachings as Stefik was interested in controlling usage rights for digital content and the multiple database system disclosed by Fox would help achieve that goal.

**Claims 5 and 14:**

Fox does not, but Stefik discloses the content comprising digital audio data (col 6, lines 48-52). Reasons one of ordinary skills would want to combine the two teachings have already been discussed.

**Claims 7 and 16:**

Fox does not teach a method and article of claims 1 and 10 respectively, wherein the first authentication code comprises a hash of the first database and a first secret, and the second authentication code comprises a hash of the second database and a second secret, the first secret being different than the second secret. However, as mentioned already, RFC 2104 discloses the use of HMAC, which uses a hash and a secret key, which are more secure than ordinary hashes or checksums. Further it is obvious to use different secret keys for the first and second authentication code as this would make the databases further secure as should somehow a hacker were to break one authentication code, he/she would still need to spend some time to break the second. One of ordinary skills would be motivated to combine the teachings of Fox and RFC 2104 according to the limitations recited in claims 7 and 16 for the same reasons given in claim 1.

**Claims 8 and 17:**

It is obvious and inherent that if the first authentication code comprises a hash of the first database and a first secret, then the portion of the first authentication code would have to comprise the first secret.

**Claims 9 and 18:**

Fox and Stefik does not specifically teach allowing a predetermined number of operations of copying the second database over the first database without presenting a challenge code to the user, requiring the user to obtain the passcode, and determining the validity of the passcode. However, it is obvious to one of ordinary skill in the art to have done so because the reason Stefik wanted to control the distribution and usage of digital content was so the owner can make a profit off the digital content. Stefik recognized that should the digital content user need to contact a central licensing facility for licensing issues all the time, someone would need to absorb the cost of communication—most likely the digital content owner (col 2, lines 44-54). Therefore, it makes sense to allow a predetermined number of copy operations of the second database over the first without presenting a challenge code to the user, as this would minimize the cost of running a central licensing facility.

Fox and Stefik does not specifically teach allowing a predetermined number of operations of copying the second database over the first database without presenting a challenge code to the user, requiring the user to obtain the passcode, and determining the validity of the passcode. However, it is obvious to one of ordinary skill in the art to have done so because the reason Stefik wanted to control the distribution and usage of

digital content was so the owner can make a profit off the digital content. Stefik recognized that should the digital content user need to contact a central licensing facility for licensing issues all the time, someone would need to absorb the cost of communication—most likely the digital content owner (col 2, lines 44-54). Therefore, it makes sense to allow a predetermined number of copy operations of the second database over the first without presenting a challenge code to the user, as this would minimize the cost of running a central licensing facility.

**Claims 19 and 25:**

Fox discloses a method of, and an article comprising a storage medium having a plurality of machine readable instructions, wherein when the machine readable instructions are executed by a processor, the machine readable instructions provide for:

- Determining if the first database is corrupted, the first database being associated with a first message authentication code (MAC) (col 1, lines 65-67 and col 2, lines 1-6).
- Determining if a second database is corrupted, the second database being associated with a second message authentication code (MAC), and having contents substantially the same as the first database (col 2, 2<sup>nd</sup> paragraph).

The examiner has interpreted an authentication code as any sort of hash, object, code, or checksum value associated with a database in any manner.

Fox does not disclose, but Stefik teaches presenting a challenge code to a user of the application program, requiring the user to obtain a passcode in response to the challenge code, and determining validity of the passcode (col 3, lines 34-50). Stefik

Art Unit: 2135

disclosed that it is possible for a user to have access to selected content already, but not be able to make any practical use of the content until they contact a central accounting facility to obtain a key/passcode to unlock the selected content. **Stefik teaches these things by disclosing that they were known in the art at the time the applicant's invention was made.** One of ordinary skill in the art at the time of the applicant's invention would be motivated to combine Stefik and Fox's teachings so that Stefik's invention of a system for controlling digital content would use at least two databases to prevent a rollback attack against the first database in accordance with the teachings of Fox as Stefik was interested in controlling the distribution and usage of digital works and a rollback attack would compromise this control. In the broadest reasonable interpretation, Table 1 as disclosed by Stefik (col 10 and 11) is a database, which is being used to keep track of usage and distribution rights. One of the items in the table/database is a field, which keeps track of the number of copies of a digital media in use (Table 1, 1<sup>st</sup> item). The number in this field is easily subject to a rollback attack.

Neither Fox nor Stefik teaches when the second database is not corrupted, recalculating the second MAC using a portion of the first MAC, copying the second database over the first database, and proceeding with authorized operations for processing content by an application program. However, RFC 2104 teaches the use of HMAC, (Key) Hashed Message Authentication Code. RFC 2104 discloses that an authentication code using a hash or checksum, such as MD5, along with a secret key can be used to provide a way "to check the integrity of information transmitted over or

stored in an unreliable medium" (RFC 2104, Introduction). One advantage of using HMAC over just an ordinary checksum algorithm is that the checksum algorithm portion of a HMAC can be replaced with a more secure or reliable algorithm discovered at a later date (RFC, 2104, Introduction). Used in combination with the secret key, it is also more inherently secure than an ordinary checksum.

One of ordinary skill in the art at the time of the applicant's invention would be motivated to use HMAC instead of an ordinary checksum as an authentication code as this would inherently make the databases more secure. One of ordinary skill would also recognize that before copying the second database over the first, the second authentication code (which would also be transmitted to the first database) would have to be recalculated using the key portion of the first authentication code's HMAC as the newly copied first database would need a new authentication code and its secret key is different than the second's secret key. Therefore, the newly calculated authentication code would have to use the first database's secret key in the calculation of a new code.

Fox discloses the use of multiple databases to ensure database integrity and it would be obvious to one of ordinary skill in the art to copy the second database only when it is not corrupted. Further, it is obvious that since Stefik is interested in the security of the digital content, to copy the database only when the passcode is also valid.

Fox discloses a method of claim 19 further comprising, and an article of claim 25, further comprising instructions for, continuing with authorized operations of the application program for processing content when the first database is not corrupted (col

Art Unit: 2135

7, lines 27-41 and fig 6). One of ordinary skill would recognize that there is no point in not doing anything if the first database is not corrupt and instead would continue with ordinary operations of the application.

Fox does not teach, but Stefik discloses the first database comprising usage rules for processing selected content by the application program, the usage rules including a copy count for the selected content (col 3, 1<sup>st</sup> paragraph; col 4, lines 4-24; and col 10 and 11, Table 1).

Stefik further discloses the content comprising digital audio data (col 6, lines 48-52). After the corruption in the first database has been fixed, it is obvious to proceed with authorized operations for processing content by the application program as the error that caused it to stop in the first place has been fixed. As both databases essentially contain the same data, both databases are associated with the application program and both contain usage rules for the digital audio content.

**Claims 20 and 26:**

Fox does not disclose, but Stefik teaches, a method of claim 19 and an article of claim 25, wherein the usage rules comprise a copy count for the digital audio content (col 6, Table 1, item 1). Motivations for combining the two teachings have been discussed already.

**Claims 22 and 27:**

Fox does not teach a method and article of claims 19 and 25 respectively, wherein the first MAC comprises a hash of the first database and a first secret, and the second MAC comprises a hash of the second database and a second secret, the first

Art Unit: 2135

secret being different than the second secret. However, as mentioned already, RFC 2104 discloses the use of HMAC, which uses a hash and a secret key, which are more secure than ordinary hashes or checksums. Further it is obvious to use different secret keys for the first and second MAC as this would make the databases further secure as should somehow a hacker were to break one MAC, he/she would still need to spend some time to break the second.

**Claims 23 and 28:**

Fox and Stefik does not specifically teach allowing a predetermined number of operations of copying the second database over the first database without presenting a challenge code to the user, requiring the user to obtain the passcode, and determining the validity of the passcode. However, it is obvious to one of ordinary skill in the art to have done so because the reason Stefik wanted to control the distribution and usage of digital content was so the owner can make a profit off the digital content. Stefik recognized that should the digital content user need to contact a central licensing facility for licensing issues all the time, someone would need to absorb the cost of communication—most likely the digital content owner (col 2, lines 44-54). Therefore, it makes sense to allow a predetermined number of copy operations of the second database over the first without presenting a challenge code to the user, as this would minimize the cost of running a central licensing facility.

**Claim 24:**

Fox does not disclose, but Stefik teaches processing the digital audio content by an application program consistent with the usage rules (col 15, lines 17-29). Stefik does

Art Unit: 2135

not teach a method of claim 19, wherein copying of the second control database over the first control database is performed after beginning execution of the application program but before proceeding with authorized operations. However, it is inherent that if Stefik's invention was to incorporate Fox's teachings to utilize two databases and to copy a second database onto a first database should the first database become corrupt, then the copying of the second database would not occur until after the beginning of the execution of the application program as the application program would check to verify the integrity of the database and authorized operations would not occur until the corruption has been fixed if one was detected, else there would be no point in attempting to detect the corruption.

### ***Conclusion***

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

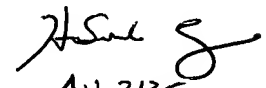
A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.



Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 8:00am-4:30pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

  
AU 2135

PP